DETAILED ACTION

Claims 1-19 are pending.

Response to Amendment

1. In view of the amendment received on 3/20/08, the rejection under 35 U.S.C. 101 to claims 18 and 19 is withdrawn.

2. In view of the amendment received on 3/20/08, the rejection under 35 U.S.C. 112 to claims 9-15, 17 and 18 is withdrawn.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. Claims 1-7 and 9-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Straumann et al. (U.S. PATENT NO. 7,196,610) in view of Kniffin et al. (U.S. PATENT NO. 6,072,402).

-Regarding claims 1 and 9, Straumann et al. disclose an access control system comprising a standard access control system **(as disclosed in fig. 1)**, having a plurality of access points, each access point being controllable by an individual physical locking mechanisms **(access control device 1 is connected to an electromechanical lock 15; the access control system comprises a plurality of access control devices 1, 1' which control access doors 3, 3' as disclosed in fig. 1 and further disclosed in col. 5 lines 44-63)** and including at least one reader and a controller for controlling the locking mechanisms **(the access control device 1 further comprises an access control module 13 as disclosed in fig. 1 and further disclosed in col. 6 lines 25-47)**, and a short-range transmitter is provided at one specified location, said short-range transmitter being an independent unit having no direct connection to the standard access control system, said transmitter being operative to transmit access-point-specific identification information for reception by a mobile telephone which is located in the reception area of the transmitter, and is used at least indirectly by this to control the access control at a specific associated access points **(the communication module 11 comprises a transceiver for wireless data communication by means of electromagnetic waves; the stored access control device identification is transmitted via the communication module 11 when the presence of an external communication terminal 2 is detected by the communication module 11 as disclosed in fig. 1 and further disclosed in col. 5 line 67-col. 6 line 18; Straumann et al. disclose the**

claimed invention except for said short-range transmitter being an independent unit having no direct connection to the standard access control system. It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the short-range transmitter to be an independent unit having no direct connection to the standard access control system, since it has been held that constructing a formerly integral structure in various elements involves only routine skill in the art. *Nerwin v. Erlichmena*, 168 USPQ 177, 179).

However, Straumann et al. fail to disclose at least one access control server, said at least one access control server being operative to carry out central management of access data and being connected to a plurality of said controllers; at least one mobile telephony server connected to the access control server, which is at least indirectly able to send data via a mobile telephone network to mobile telephone subscribers, and to receive data from mobile telephone subscribers.

Kniffin et al. disclose at least one access control server, said at least one access control server being operative to carry out central management of access data and being connected to a plurality of said controllers **(clearinghouse 54 transmits an RF signal to the identified lock and causes it to briefly make itself susceptible to being unlocked as disclosed in fig. 3 and further disclosed in col. 7 lines 20-30)**; at least one mobile telephony server connected to the access control server, which is at least indirectly able to send data via a

mobile telephone network to mobile telephone subscribers, and to receive data from mobile telephone subscribers **(RF transmission system is connected to the clearinghouse and receiving calls from the cellular telephone 52 as disclosed in fig. 3 and further disclosed in col. 7 lines 20-21)**.

Therefore, it would have been obvious to one of ordinary skills in the art at the time of invention to modify the access control device as disclosed by Straumann et al. to connect to an access control server (clearinghouse) as disclosed by Kniffin et al. One is motivated as such in order to provide a central monitoring system for improving security.

-Regarding claims 2 and 10, the combination further discloses the specified location is a location in the area of the associated access point, such that the identification information from the transmitter can be received by the mobile telephone only in the immediate vicinity of the access points **(Straumann et al., the communication module 11 is located in the area of the associated access point as disclosed in fig. 1 and the communication module 21 is activated by the user of the mobile communication terminal 2 in the vicinity of the access control device 1 to be passed as disclosed in col. 8 lines 14-16)**.

-Regarding claim 3, the combination further discloses the specified location is a location in front of the associated access points **(Straumann et al., as disclosed in fig. 1)**.

-Regarding claim 4, the combination further discloses the transmitter is a Bluetooth appliance **(Straumann et al., the communication module 11 comprises a Bluetooth transceiver for wireless data communication by means of electromagnetic waves as disclosed in col. 6 line 5)**, with a range of less than 10 meters **(it is inherent for the Bluetooth range to be less than 10 meters)**, and wherein the authorized mobile telephone has a Bluetooth interface **(Straumann et al., the communication module 21 is corresponding to the communication module 11 for data exchange with the access control devices 1 as disclosed in col. 6 lines 62-65)**.

-Regarding claim 5, the combination of Straumann et al. and Kniffin et al. teaches all the limitations as claimed in claim 1. Straumann et al. disclose the communication module 11 comprises a transceiver for wireless data communication by means of electromagnetic waves in col. 6 lines 1-5 and the communication module 21 is corresponding to the communication module 11 for data exchange with the access control devices 1 as disclosed in col. 6 lines 62-65. Even thought the combination does not specifically disclose the interface is WLAN, it would have been obvious to one of ordinary skills in the art at the time of invention to modify the interface to be WLAN. One is motivated as such in order to provide for a cost efficient and ease of integration system.

-Regarding claim 6, the combination further discloses the identification information is one of a hardware-specific, unique address of the transmitter, an appliance-specific 48-bit address of a Bluetooth appliance **(it is inherent for**

each Bluetooth appliance to have a unique 48-bit address and use the address for connecting to other Bluetooth device).

-Regarding claim 7, the combination further discloses the transmitter is in the form of an independent unit, which preferably has no direct connection to the mobile telephony server **(Straumann et al., communication module 11 is not direct connected to the mobile telephony server as disclosed in fig. 1)**.

-Regarding claim 11, the combination further discloses after detection of the identification information **(Straumann et al., the communication module 21 is activated by the user of the mobile communication terminal 2 in the vicinity of the access control device 1 to be passed as disclosed in col. 8 lines 14-16)**, the mobile telephone additionally demands the input of user-specific authentication information is transmitted together with the identification of the access point to be processed via the mobile telephone network to the mobile telephony server and to the access control server, which then activates the associated controller **(Kniffin et al., as disclosed in col. 2 lines 31-43)**.

-Regarding claims 12, 18 and 19, the combination further discloses the mobile telephone transmits the identification information and if appropriate the PIN code **(Kniffin et al., PIN number is provided by the user using a telephone's touch tone pad 22 as disclosed in col. 2 lines 42-43)** via the GSM network in the form of a telephonic data transmission **(Straumann et al., the mobile radio network 5 is a GSM network as disclosed in col. 6 lines 58-61)**.

-Regarding claim 13, the combination further discloses the transmitter is a Bluetooth appliance **(Straumann et al., the communication module 11 comprises a Bluetooth transceiver for wireless data communication by means of electromagnetic waves as disclosed in col. 6 line 5)**, which transmits its unique address as identification information, and this address is used to identify the associated access point **(it is inherent for each Bluetooth appliance to have a unique 48-bit address and use the address for connecting to other Bluetooth device when they are in range)**, and wherein the mobile telephone has a Bluetooth interface **(Straumann et al., the communication module 21 is corresponding to the communication module 11 for data exchange with the access control devices 1 as disclosed in col. 6 lines 62-65)**, in which case the mobile telephone automatically starts an appropriate dialogue with the mobile telephone user on reception of specific addresses of this type which are transmitted in the course of the authorization process and correspond to the authorized access points **(Kniffin et al., the user establishes communication to a clearinghouse 18, a series of voice prompts synthesized by a computer 20 at the clearinghouse and relayed to the user over the link 16 solicits the user to identify the lock 12 to which access is desire (the lock is usually identified by a number, in this case, the lock is identified by the Bluetooth address gathered by the communication module 21 as disclosed by Straumann et al.) as disclosed in col. 2 lines 31-40)**, possibly requests authentication of the user, and in any case then transmits

a request to open the specific access point via the mobile telephone network to the mobile telephony server and to the access control server **(Kniffin et al., as disclosed in col. 2 lines 31-43)**.

-Regarding claim 14, the combination of Straumann et al. and Kniffin et al. teaches all the limitations as claimed in claim 1. Straumann et al. disclose the combination further discloses the transmitter is a Bluetooth appliance **(Straumann et al., the communication module 11 comprises a Bluetooth transceiver for wireless data communication by means of electromagnetic waves as disclosed in col. 6 line 5)**. Even thought the combination does not specifically disclose the transmitter is arranged in the area of a gateway, and wherein the identification information can be received by a mobile telephone only within a distance of less than 1 m outside and in front of the gateway, it would have been obvious to one of ordinary skills in the art at the time of invention to do so. One is motivated as such in order to provide for power conservation by limiting the range of Bluetooth transmitter to 1 m.

-Regarding claim 15, the combination further discloses the transmitter is a Bluetooth appliance **(Straumann et al., the communication module 11 comprises a Bluetooth transceiver for wireless data communication by means of electromagnetic waves as disclosed in col. 6 line 5)**, which is arranged in a specific area in front of the associated access point **(Straumann et al., the communication module 11 is located in the area of the associated access point as disclosed in fig. 1 and the communication module 21 is**

activated by the user of the mobile communication terminal 2 in the vicinity of the access control device 1 to be passed as disclosed in col. 8 lines 14-16).

-Regarding claim 16, Kniffin et al. disclose a access recording system having a standard access recording system which comprises at least one access recording server which carries out central management of the access data **(the secure access system to record data relating to lock access as disclosed in col. 4 lines 52-53 and the access log data is RF-transmitted to the clearinghouse as disclosed in col. 5 lines 3-4)**; at least one mobile telephony server operative in conjunction with the access recording server, which is at least indirectly able to transmit data via a mobile telephone network to mobile telephone subscribers **(RF transmission system is connected to the clearinghouse and receiving calls from the cellular telephone 52 as disclosed in fig. 3 and further disclosed in col. 7 lines 20-21)**; and a proximity detector **(as disclosed in col. 3 lines 50-63).** However, Kniffin et al. does not specifically point out the access data comprises time data and the proximity detector is a short-range transmitter provided for at least one authorized areas, which transmitter is in the form of an independent unit, with no direct connection to the standard time recording system, and is operative to transmit area-specific identification information in such a way that the information is received only by a mobile telephone which is located in the immediate vicinity of the authorized

area, and is used by said mobile telephone at least indirectly for the manipulation of the time data.

Straumann et al. disclose time determination module 14 for determining current time indications; and a short-range transmitter **(the communication module 11 comprises a Bluetooth transceiver for wireless data communication by means of electromagnetic waves as disclosed in col. 6 line 5)** provided for at least one authorized areas, which transmitter is in the form of an independent unit, with no direct connection to the standard time recording system, and is operative to transmit area-specific identification information in such a way that the information is received only by a mobile telephone which is located in the immediate vicinity of the authorized area, and is used by said mobile telephone at least indirectly for the manipulation of the time data **(the communication module 11 is located in the area of the associated access point as disclosed in fig. 1 and the communication module 21 is activated by the user of the mobile communication terminal 2 in the vicinity of the access control device 1 to be passed as disclosed in col. 8 lines 14-16; Straumann et al. disclose the claimed invention except for said short-range transmitter being an independent unit having no direct connection to the standard access control system. It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the short-range transmitter to be an independent unit having no direct connection to the standard access control system, since it has been held**

that constructing a formerly integral structure in various elements involves only routine skill in the art. *Nerwin v. Erlichmena*, 168 USPQ 177, 179), and is used by this mobile telephone at least indirectly for the manipulation of the time data **(the communication module 21 is activated by the user of the mobile communication terminal 2 in the vicinity of the access control device 1 to be passed as disclosed in col. 8 lines 14-16)**.

Therefore, it would have been obvious to one of ordinary skills in the art at the time of invention to modify the access data as disclosed by Kniffin et al. to include the time data as disclosed by Straumann et al. One is motivated as such in order to provide a complete access data log for improving the security record. It would have been obvious to one of ordinary skills in the art at the time of invention to further modify the proximity detector as disclosed by Kniffin et al. to be a short-range transmitter as disclosed by Straumann et al. One is motivated as such in order to provide for power conservation by using a low power transmitter such as Bluetooth transmitter.

-Regarding claim 17, Kniffin et al. disclose a method for time recording, using a time recording system having a standard time recording system with at least one time recording server carrying out central management of the time data **(the secure access system to record data relating to lock access as disclosed in col. 4 lines 52-53 and the access log data is RF-transmitted to the clearinghouse as disclosed in col. 5 lines 3-4)**, at least one mobile telephony server in conjunction with the time recording server, at least indirectly

transmitting data via a mobile telephone network to mobile telephone subscribers **(RF transmission system is connected to the clearinghouse and receiving calls from the cellular telephone 52 as disclosed in fig. 3 and further disclosed in col. 7 lines 20-21)**; and transmitting time data to the time recording server, and/or checking by the server, via the mobile telephone, the mobile telephone network and the mobile telephony server **(the user operates the cellular telephone 52 to call the clearing house 54 and request access to a particular lock 56 as disclosed in fig. 3 and further disclosed in col. 7 lines 20-22)**. However, Kniffin et al. fail to disclose a short-range transmitter is provided for at least one authorized area, which transmitter is in the form of an independent unit, with no direct connection to the standard time recording system and is operative to transmit area-specific identification information in such a way that the information is received only by a mobile telephone which is located in the immediate vicinity of the authorized area, and is used by said mobile telephone at least indirectly for the manipulation of the time data, and a mobile telephone is authorized to input time data in specific authorized areas, in at least one specific time period, via the time recording server and via the mobile telephony server via the mobile telephone network, transmitting by the transmitter area-specific identification information continuously or at times, in such a manner that it can received only by a mobile telephone which is located in the immediate vicinity of the authorized area, and detecting by a mobile telephone which is located in the

immediate vicinity of the area detects the identification of this area via this identification information.

Straumann et al. disclose a short-range transmitter is provided for at least one authorized area, which transmitter is in the form of an independent unit, with no direct connection to the standard time recording system and is operative to transmit area-specific identification information in such a way that the information is received only by a mobile telephone which is located in the immediate vicinity of the authorized area, and is used by said mobile telephone at least indirectly for the manipulation of the time data **(the communication module 11 is located in the area of the associated access point as disclosed in fig. 1 and the communication module 21 is activated by the user of the mobile communication terminal 2 in the vicinity of the access control device 1 to be passed as disclosed in col. 8 lines 14-16; Straumann et al. disclose the claimed invention except for said short-range transmitter being an independent unit having no direct connection to the standard access control system. It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the short-range transmitter to be an independent unit having no direct connection to the standard access control system, since it has been held that constructing a formerly integral structure in various elements involves only routine skill in the art. *Nerwin v. Erlichmena*, 168 USPQ 177, 179)**, and a mobile telephone is authorized to input time data in specific authorized areas, in at least one specific

time period, via the time recording server and via the mobile telephony server via the mobile telephone network **(stored, assigned in each case to the access control device identification for an access control device 1, in the data store of the access authorization module 221 are the access code for the respective access control device 1 and access rights data, which define time periods during which the user can be granted access to the object controlled by the respective access control device 1 as disclosed in col. 7 lines 9-30)**, transmitting by the transmitter area-specific identification information continuously or at times, in such a manner that it can received only by a mobile telephone which is located in the immediate vicinity of the authorized area **(the communication module 11 is located in the area of the associated access point as disclosed in fig. 1 and the communication module 21 is activated by the user of the mobile communication terminal 2 in the vicinity of the access control device 1 to be passed as disclosed in col. 8 lines 14-16)**, and detecting by a mobile telephone which is located in the immediate vicinity of the area detects the identification of this area via this identification information **(it is inherent for each Bluetooth appliance to have a unique 48-bit address and use the address for connecting to other Bluetooth device)**.

Therefore, it would have been obvious to one of ordinary skills in the art at the time of invention to modify the access data as disclosed by Kniffin et al. to include the time data as disclosed by Straumann et al. One is motivated as such in order to provide a complete access data log for improving the security record.

It would have been obvious to one of ordinary skills in the art at the time of invention to further modify the proximity detector as disclosed by Kniffin et al. to be a short-range transmitter as disclosed by Straumann et al. One is motivated as such in order to provide for power conservation by using a low power transmitter such as Bluetooth transmitter.

4. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Straumann et al. (U.S. PATENT NO. 7,196,610) in view of Kniffin et al. (U.S. PATENT NO. 6,072,402) and further in view of Want et al. (U.S. PG-PUB NO. 2003/0114104).

-Regarding claim 8, the combination of Straumann et al. and Kniffin et al. teaches all the limitations as claimed in claim 1. Straumann et al. disclose the communication module 11 comprises a transceiver for wireless data communication by means of electromagnetic waves in col. 6 lines 1-5 and the communication module 21 is corresponding to the communication module 11 for data exchange with the access control devices 1 as disclosed in col. 6 lines 62-65. However, the combination fails to disclose the standard access control system also allows access control using RFID technology.

Want et al. disclose each portable electronic device 14, 16, 18 includes a radio frequency identification (RFID) tag 24 and, accordingly, the computer access device 12 includes a complimentary RFID reader 26 as disclosed in fig. 1 and paragraph 11.

Therefore, it would have been obvious to one of ordinary skills in the art at the time of invention to modify the interface to be RFID. One is motivated as such in order to provide for ease of operating the system.

Response to Arguments

5. Applicant's arguments filed 3/20/08 have been fully considered but they are not persuasive.

a. In pages 9-14 of the remarks, regarding claims 1-7 and 9-19, applicant argues that the access control server of the present invention is in direct contact with the local controllers; and a short range transmitter, in the form of an independent unit with no direct connection to the standard access control system, is provided at one specified location.

-The examiner respectfully disagrees. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Also, the access control server (clearinghouse) is indeed in direct contact with the local controllers (lock) through RF transmission as disclosed in Kniffin et al. fig. 3 and col. 7 lines 20-25. Furthermore, although Straumann et al. disclose the claimed invention except for said short-range transmitter being an independent unit having no direct connection to the standard access control system, it would have

been obvious to one having ordinary skill in the art at the time the invention was made to modify the short-range transmitter to be an independent unit having no direct connection to the standard access control system, since it has been held that constructing a formerly integral structure in various elements involves only routine skill in the art. *Nerwin v. Erlichmena*, 168 USPQ 177, 179.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PING Y. HSIEH whose telephone number is (571)270-

3011. The examiner can normally be reached on Monday-Thursday (alternate Fridays) 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lana Le can be reached on 571-272-7891. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/P. Y. H./
Examiner, Art Unit 2618

/Lana N. Le/
Acting SPE of Art Unit 2618